STATE OF ALABAMA

Information Technology Guideline

Guideline 660-02G6: Domain Name System (DNS) Security

1. INTRODUCTION:

The resolution of domain names on the Internet is critically dependent on the proper, safe, and secure operation of the domain name system (DNS). Deployment guidelines for secure DNS broadly consist of the following recommendations:

Implement appropriate system and network security controls for securing the DNS hosting environment, such as operating system and application patching, process isolation, and network fault tolerance.

Protect DNS transactions such as update of DNS name resolution data and data replication that involve DNS nodes within an enterprise's control. The transactions should be protected using hash-based message authentication codes based on shared secrets, as outlined in the Internet Engineering Task Force's (IETF) Transaction Signature (TSIG) specification.

Protect DNS query/response transactions (that could involve any DNS node in the global Internet) using digital signatures based on asymmetric cryptography as outlined in IETF's Domain Name System Security Extensions (DNSSEC) specification.

Enforce content control of DNS name resolution data using a set of integrity constraints that provide the right balance between performance and integrity of the DNS system.

Establish a secure baseline configuration and manage it securely from that point forward by monitoring DNS transactions, planning for contingencies, and implementing administrative controls to ensure the integrity and availability of the DNS infrastructure.

2. OBJECTIVE:

The primary security goals for DNS are data integrity and source authentication, which are needed to ensure the authenticity of domain name information and maintain the integrity of domain name information in transit.

3. SCOPE:

These guidelines cover secure configuration and operation of domain name systems serving the alabama.gov and al.state.us domains (zones). The target audience consists of zone administrators who are responsible for the configuration and operation of these name servers.

4. GUIDELINES:

The following guidelines, based on the recommendations of the National Institute of Standards and Technology (NIST) in Special Publication 800-81: Secure Domain Name System (DNS) Deployment Guide, should be used to secure the State of Alabama DNS infrastructure.

4.1 SECURE DNS HOSTING ENVIRONMENT

Ensure the platform on which the DNS software runs contains no programs other than those needed for operating system and network support. Likewise, DNS software should not be running or present on hosts that are not designated as name servers.

A name server instance should always be configured as either an authoritative name server or a resolving name server. An authoritative name server should have recursion turned off.

The authoritative name servers for an enterprise should be both network and geographically dispersed. Network-based dispersion consists of ensuring that all name servers are not behind a single router or switch, in a single subnet, or using a single leased line. Geographic dispersion consists of ensuring that not all name servers are in the same physical location, and hosting at least a single secondary server off-site.

For split DNS implementation, there should be a minimum of two physical files or views. One should exclusively provide name resolution for hosts located inside the firewall. It also can contain resource record (RR) sets for hosts outside the firewall. The other file or view should provide name resolution only for hosts located outside the firewall or in the DMZ, and not for any hosts inside the firewall.

When installing an upgraded version of name server software, the administrator should make necessary changes to configuration parameters to take advantage of new security features.

Whether running the latest version [of BIND (Berkeley Internet Name Domain)] or an earlier version, the administrator should be aware of the vulnerabilities, exploits, security fixes, and patches for the version that is in operation in the enterprise. The following actions are recommended:

- Join the Internet Systems Consortium (ISC) BIND forum https://www.isc.org/software/guild/bf
- Periodically refer to the BIND vulnerabilities page at http://www.isc.org/software/bind/security
- Refer to CERT®/CC's Vulnerability Notes Database at http://www.kb.cert.org/vuls/ and the NIST National Vulnerability Database (NVD) at http://nvd.nist.gov/

To prevent the release of information about which version of BIND is running on a system, name servers should be configured to refuse queries for "version.bind".

4.2 SECURE DNS TRANSACTIONS

It is recommended that the administrator create a named list of trusted hosts (or blacklisted hosts) for each of the different types of DNS transactions. In general, the role of the following categories of hosts should be considered for inclusion in the appropriate access control list (ACL):

- DMZ hosts defined in any of the zones in the enterprise
- All secondary name servers allowed to initiate zone transfers

- Internal hosts allowed to perform recursive queries

The process of authenticating the source of a message and its integrity through hash-based message authentication codes (HMAC) is specified through a set of DNS specifications known collectively as TSIG. The following recommendations apply to TSIG:

The TSIG key should be a minimum of 128 bits in length.

A unique TSIG key should be generated for each pair of communicating hosts (i.e., a separate key for each secondary name server to authenticate transactions with the primary name server, etc.)

After the key string is copied to the key file in the name server, the two files generated by the dnssec-keygen program should either be made accessible only to the server administrator account (e.g., root in Unix) or, better still, deleted. The paper copy of these files also should be destroyed.

The key file should be securely transmitted across the network to name servers that will be communicating with the name server that generated the key.

The statement in the configuration file (usually found at /etc/named.conf for BIND running on Unix) that describes a TSIG key (key name [ID], signing algorithm, and key string) should not directly contain the key string. When the key string is found in the configuration file, the risk of key compromise is increased in some environments where there is a need to make the configuration file readable by people other than the zone administrator. Instead, the key string should be defined in a separate key file and referenced through an include directive in the key statement of the configuration file. Every TSIG key should have a separate key file.

The key file should be owned by the account under which the name server software is run. The permission bits should be set so that the key file can be read or modified only by the account that runs the name server software.

The TSIG key used to sign messages between a pair of servers should be specified in the server statement of both transacting servers to point to each other. This is necessary to ensure that both the request message and the transaction message of a particular transaction are signed and hence secured.

4.3 SECURE DNS QUERY/RESPONSE

Name servers that deploy DNSSEC signed zones or query signed zones should be configured to perform DNSSEC processing.

The key size for the Key Signing Key (KSK) should be sufficiently large (2048 bit) because of the greater impact on DNS due to KSK key compromise.

The private keys corresponding to both the Zone Signing Key (ZSK) and the KSK should not be kept on the DNSSEC-aware primary authoritative name server when the name server does not support dynamic updates. If dynamic update is supported, the private key corresponding to the ZSK alone should be kept on the name server, with appropriate directory/file-level access control list-based or cryptography-based protections.

Signature generation using the KSK should be done offline, using the KSK-private stored offline; then the DNSKEY RRSet, along with its resource record signature (RRSIG) RR, can be loaded into the primary authoritative name server.

4.4 DNS DATA CONTENT CONTROL

The refresh value in the zone Start of Authority (SOA) RR should be chosen with the frequency of updates in mind. If the zone is signed, the refresh value should be less than the RRSIG validity period.

The retry value in a zone SOA RR should be 1/10th of the refresh value.

The expire value in the zone SOA RR should be 2 to 4 weeks.

The minimum TTL value should be between 30 seconds and 24 hours.

A DNS administrator should not include in a zone file host information (HINFO), location (LOC), Responsible Person (RP), or other RR types that could divulge information that would be useful to an attacker, or the external view of a zone if using split DNS.

A DNS administrator should review the data contained in any text (TXT) RR for possible information leakage before adding it to the zone file.

The validity period for the RRSIGs covering a zone's DNSKEY RRSet should be in the range of 2 days to 1 week. This value helps reduce the vulnerability period resulting from a key compromise.

A zone with delegated children should have a validity period of a few days to 1 week for RRSIGs covering the Delegation Signer (DS) RR for a delegated child. This value helps reduce the child zone's vulnerability period resulting from a KSK compromise.

4.5 DNS SECURITY ADMINISTRATION OPERATIONS

This section deals with periodic security administration operations (and associated checklists) in a DNSSEC-aware enterprise-level zone and how to perform those operations securely.

The KSK needs to be rolled over less frequently than the ZSK. The recommended rollover frequency for the KSK is once a year (with a size of 2048 bits using RSA/SHA1), whereas the ZSK should be rolled over every month (with a key size of 1024 bits using RSA/SHA1).

Zones that pre-publish the new public key should observe the following:

- The secure zone that pre-publishes its public key should do so at least one TTL period before the time of the key rollover.
- After removing the old public key, the zone should generate a new signature (RRSIG RR), based on the remaining keys (DNSKEY RRs) in the zone file.

A DNS administrator should have the emergency contact information for the immediate parent zone to use when an emergency KSK rollover must be performed.

A parent zone must have an emergency contact method made available to its delegated child subzones in case of emergency child subzone KSK rollover. There also should be a secure means of obtaining the subzone's new KSK.

To reduce the useful time period for a compromised KSK, the RRSIG validity period over the DS RRset in the parent zone should be kept as short as possible. A suggested validity period would be 2 to 4 days, with 7 days maximum.

Periodic re-signing should be scheduled before the expiration field of the RRSIG RRs found in the zone. This is to reduce the risk of a signed zone being rendered bogus because of expired signatures.

The serial number in the SOA RR must be incremented before re-signing the zone file. If this operation is not done, secondary name servers may not pick up the new signatures because they are refreshed purely on the basis of the SOA serial number mismatch. The consequence is that some security-aware resolvers will be able to verify the signatures (and thus have a secure response) but others cannot.

4.6 CONFIGURATION OF WINDOWS 2000/2003 DNS

The following guidelines, adapted from the Defense Information Systems Agency (DISA) DNS Security Technical Implementation Guide (STIG) Version 4 Release 1, apply to Windows 2000/2003 DNS implementations.

4.6.1 Secure Dynamic Updates and Active Directory

Disable the DHCP server service on any Windows 2000/2003 DNS server that supports dynamic updates.

Ensure computer accounts for DHCP servers are not members of the DNSUpdateProxy group.

4.6.2 Zone Transfers

Configure Windows 2000/2003 DNS to prohibit zone transfers or implement a VPN solution that requires cryptographic authentication of communicating devices and is used exclusively by name servers authoritative for the zone.

4.6.3 Forwarders and Recursion

Disable forwarders on an authoritative Windows 2000/2003 DNS server.

Disable recursion on an authoritative Windows 2000/2003 DNS server.

4.6.4 WINS Integration

Configure Windows 2000/2003 DNS to prohibit WINS lookup.

4.6.5 Logging

The DNS service should log success and failure of the following:

- Start and stop of the DNS service
- Zone transfers

- Zone update notifications
- Dynamic updates
- Queries

Events related to DNS service start and stop appear in the Windows 2000 System Event Log. Other events are logged to a file named "%systemroot%\system32\dns\dns.log."

Windows 2000 DNS has its own logging facility, which is primarily designed to debug DNS problems rather than maintain a record of DNS transactions. The Windows 2003 logging tab has been split into two; debugging and event logging. To implement the general logging requirements listed above, the DNS software administrator must select the "Query," "Notify," and "Update" debug logging options.

4.6.6 IPv6 and Windows DNS

Ensure the IPv6 protocol is not installed if the server is only configured to respond to IPv4 A records.

4.7 STANDARD OPERATING REQUIREMENTS

4.7.1 Personnel

Ensure at least one backup DNS database administrator is identified for each supported zone and at least one backup DNS software administrator is identified for each name server.

4.7.2 Physical Access Control

Name servers should be among the most secured computers/assets at a location because compromise of a name server can directly impact the security of the services it supports. Ensure a name server is protected by equivalent or better physical access controls than the clients it supports.

The specific area in which the name server is located must have positive access control. At a minimum, control measures should include mechanical or electronic locks. The number of individuals permitted access to the area must be limited, controlled, and recorded.

4.7.3 Business Continuity

Business continuity plans must include DNS.

Ensure that an off-site copy of zone information exists to prevent complete loss of records in the event of a disaster.

Name servers should have Uninterruptible Power Supply (UPS) or alternative power source similar to the hosts that they support.

4.7.4 Vulnerability Management

Maintain a secure system configuration in accordance with state vulnerability management standards.

4.7.5 Backup

Name servers should be backed up to external media on a regular basis. Backups should occur as frequently as needed to capture changes on the name server. Ensure, at a minimum, that DNS configuration, keys, zones, and resource record data is backed up on any day on which there are changes.

4.7.6 Cryptographic Key Supersession

Ensure cryptographic keys used to secure DNS transactions are changed at least annually.

Establish written procedures for the replacement of cryptographic keys used to secure DNS transactions that will cover, at a minimum:

- Frequency of key supersession
- Criteria for triggering emergency supersession events
- Notification of relevant personnel during emergency and non-emergency supersession
- Methods for securely transferring newly generated keys. Possibilities (in rough order of preference) are as follows:
  - SSH
  - Encrypted e-mail using PKI certificates
  - Secure fax
  - Regular mail
  - Hand courier

4.7.7 Log Archival and Review

Ensure DNS log archival requirements meet or exceed the log archival requirements of the operating system on which the DNS software resides.

Review DNS logs daily or employ a real-time log analysis or network management tool that immediately alerts an administrator of critical DNS system messages.

4.7.8 DNS Database Administration

To best assure the integrity of zone files, requests to change the DNS records should be carefully managed and the records should be checked periodically to ensure their validity.

Establish written procedures for the following:

- The process for updating zone records
- Who is authorized to submit and approve update requests
- How the DNS database administrator verifies the identity of the requester
- How the DNS database administrator documents any changes made

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 660-02: System Security
http://isd.alabama.gov/policy/Policy_660-02_System_Security.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Information Technology Standard 670-03S1: Vulnerability Management
http://isd.alabama.gov/policy/Standard_670-03S1_Vulnerability_Management.pdf

DISA DNS STIG
http://iase.disa.mil/stigs/stig/index.html

RFC 2870: Root Name Server Operational Requirements. This RFC lists mandates for root servers, but its guidance should be of interest to anyone with responsibility for a name server at any level in the DNS hierarchy. DNS administrators should review this document.
http://www.ietf.org/rfc/rfc2870.txt

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY

Version	Release Date	Comments
Original	8/21/2008	